



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/445,132	03/13/2000	AHMET MURSIT ESKICIOGLU	RCA88637	9525

24498 7590 03/31/2005

THOMSON LICENSING INC.
PATENT OPERATIONS
PO BOX 5312
PRINCETON, NJ 08543-5312

EXAMINER

KIM, JUNG W

ART UNIT PAPER NUMBER

2132

DATE MAILED: 03/31/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/445,132	Applicant(s) ESKICIOGLU ET AL.	
	Examiner Jung W Kim	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 14 March 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-20 have been examined.

Response to Amendment

2. Applicant's request for reconsideration of the finality of the rejection of the last Office action is persuasive and, therefore, the finality of that action is withdrawn.
3. Applicant's arguments, see amendment, filed March 14, 2005, with respect to the rejection(s) of claim(s) 1-20 under 35 U.S.C. 103(a) have been fully considered and are persuasive. Therefore, the rejections have been withdrawn. However, upon further consideration, a new ground(s) of rejections is made in view of Schneier.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 1-10 are rejected under 35 U.S.C. 112, first paragraph, because the specification, while being enabling for a method for managing access between a service provider and a set-top box having a smart card coupled thereto (applicant's specification, pgs. 5-12), does not reasonably provide enablement for a method for managing access to a device. The specification does not enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make or use the invention commensurate in scope with these claims. The claimed invention is much

broader than the enabling portion of the specification; for example, the specification does not enable a method for managing access to non-set top box devices, such as hand held palms or mobile phones, or in transactions between computing devices incorporating other secure protocols such as IPsec.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-10 are rejected under 35 U.S.C. 101 because they are not tangibly embodied since none of the steps define the use of network hardware to actuate the handshake method. Further, the language of the claim raises the question as to whether the claim is directed merely to an abstract idea that is not tied to a technological art, environment or machine which would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C. 101.

Claim Rejections - 35 USC § 103

7. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

8. Claims 1-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, Applied Cryptography, Chapter 3, "Basic Protocols" and Chapter 24 "Example Implementations" (hereinafter Schneier).

9. As per claims 1, 3 and 4, Schneier discloses a method for managing access to a device (pgs. 53-54, "Authentication Using Public-Key Cryptography", especially, first four steps), the method comprising:

- a. sending a first message from a first device to a second device (pg. 54, step 1; implicit in the teaching of the two parties "the host" and "Alice" are network devices configured as a sender and receiver of a secured transmission);
- b. receiving from the second device at the first device the first message encrypted using a second private key of the second device (pg. 54, steps 1 and 2);
- c. authenticating the second device in response to the first encrypted message, wherein the step of authenticating comprises the steps of:
 - i. decrypting the first encrypted message using the second public key to generate a first decrypted message; and comparing the first decrypted message to the first message (pg. 54, steps 3 and 4); and
- d. establishing a communication channel between the first and second device in response to the authentication of the second device (pg. 54, step 4; Alice has access to the host's system in response to a successful authentication of Alice).

10. The authentication scheme does not disclose the use of digital certificates wherein the certificate comprises second identification data associated with the second device and a second public key of the second device, wherein the second device encrypts the digital certificate using a first private key of the second device, and wherein the step of authenticating includes the step of decrypting the digital certificate at the first device using a first public key then using the second public key of the second device to decrypt the first encrypted message. Schneier discloses the use of digital certificates wherein the certificate comprises identification data associated with a party and a public key of a party, wherein once a received digital certificate is authenticated, the public key stored in the digital certificate is validated and used for cryptographic processing. Schneier, pg. 574, last sentence; pg. 575-576 'Certificates', especially 3rd full paragraph; the authentication of the certificate requires a first private key to seal and sign the certificate and a first public key to authenticate the certificate. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made to use a digital certificate to certify a public key, wherein prior to using the certified public key, the digital certificate is authenticated using a public key to verify the signature on the digital certificate since it certifies a specific public key with a specific user. Schneier, pg. 575, 1st full paragraph. The aforementioned cover the limitations of claims 1, 3 and 4.

11. As per claim 2, the rejections of claims 1, 3 and 4 are incorporated herein. In addition, first identification is a necessary feature of a first message to establish a secure communication by means of an authenticated handshake. Although Schneier

Art Unit: 2132

does not expressly teach including a data and a timestamp in the first message in the example disclosed, it is notoriously well-known in the art at the time the invention was made to incorporate a timestamp and date within a transmitted message. Examiner takes Official Notice of this teaching. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made for the first message to further comprise a time stamp and date since this feature prevents the message from being used in a replay attack as known to one of ordinary skill in the art. The aforementioned cover the limitations of claim 2.

12. As per claim 5, the rejections of claims 1, 3 and 4 are incorporated herein. In addition, since the first public key is available in the public domain, it would be obvious at the time the invention was made to store the first public key in the first device since it eliminates secure retrieval of the second device's public key for each secure connection between the first and second device as known to one of ordinary skill in the art. MPEP 2144.04.II. The aforementioned cover the limitations of claim 5.

13. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, and further in view of Ohashi et al. U.S. Patent No. 5,761,309 (hereinafter Ohashi).

14. As per claim 11, the rejections of claims 1-5 are incorporated herein. Schneier does not teach the method as managing access between a service provider and a set-

top box having a smart card coupled thereto, wherein authentication occurs between the set-top box and a smart card and then a set-top box and a service provider. Arnold discloses a method for authenticating a cryptographic link between a service provider and a client terminal using a smart card coupled thereto by means of certificate authentication. (Ohashi, figures 2-4 and 7-10, and related text) It would be obvious to one of ordinary skill in the art at the time the invention was made to integrate the challenge routine covered by Schneier in a connected system between a service provider and a set-top box authenticated with a smart card since it enables services provided by the service provider to be restricted based on user rights and privileges stored on the smart card and actuated by a set-top box. Ohashi, *ibid*. The aforementioned cover the limitations of claim 11.

15. Claims 12-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Ohashi, and further in view of Force et al. U.S. Patent No. 5,533,123 (hereinafter Force).

16. As per claims 12-20, the rejections of claims 1-5 and 11 under 35 U.S.C. 103(a) are incorporated herein. Schneier does not expressly disclose the smart card comprising a plurality of digital certificates, each certificate containing service provider identification. Force discloses a smart card designed to incorporate multiple types of information, including a plurality of certificates, each certificate identifying a distinct service. (Force, col. 3:22-31) It would be obvious to one of ordinary skill in the art at the

time the invention was made for the smart card to carry a plurality of certificates, wherein each certificate contains service provider information since it enables access to a plurality of services using only one smart card. Force, *ibid.* Moreover, in the ISO Authentication framework, independent certificate authorities issue digital certificates (Schneier, pg. 575, 1st full paragraph; Figure 24.3); and digital signatures in the ISO framework are tamper-resistant by means of an issuer signature on a hash of the certificate (digital certificates are secure in the public domain); hence, storage of a digital certificate at the service provider is an obvious enhancement since it eliminates the retrieval of the certificate by the provider for each authentication handshake with a set-top box. MPEP 2144.04.II. The aforementioned cover the limitations of claims 12-20.

Allowable Subject Matter

17. The subject matter defined in claims 6-10 is not covered by the teachings of the prior art of record. However, due to the 35 U.S.C. 112, 1st paragraph and 101 issues, set forth in this Office action, the claims as recited have not been found to be patentably distinct.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (571) 272-3804. The examiner can normally be reached on M-F 9:00-5:00.

Art Unit: 2132

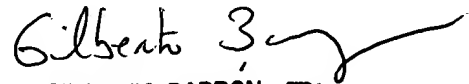
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Jung W Kim
Examiner
Art Unit 2132

Jk
March 24, 2005



GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100